REMARKS

The Office Action of October 16, 2008 has been received and carefully reviewed. It is submitted that, by this Amendment, all bases of rejection are traversed and overcome. Upon entry of this Amendment, claims 1, 4-23, 25, 26 and 28-49 remain in the application. Claims 2, 3, 24 and 27 are cancelled herein without prejudice. Reconsideration of the claims is respectfully requested.

35 U.S.C. § 102(e) rejection

Claims 1-5, 12, 20-22 and 34 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Smith et al. (U.S. Patent Publ. No. 2008/0055158).

Regarding Claim 1, the Examiner states, *inter alia*, that Smith transmits "a network management message, using one of simple network management protocol (SNMP) … over a network to a network device." The Examiner notes that in Smith paragraph [0116], the system sends alert or alarm messages using the SNMP protocol.

Smith does not teach network management messages

Applicant does not agree with the Examiner's assertions regarding Smith. For example, Applicant submits that Smith's alarm message is **not** a network management message. Smith provides as an example of the alarm message, "an asset of a certain class travels outside a predefined area." (See Smith paragraph [0097].)

In sharp contrast, a network management message as disclosed by Applicant would not include Smith's alarm (which is more like a theft alarm than a network management message). Applicant's network management messages cause network attached devices to send responses, which responses are collected and analyzed using a Kalman filter. For example, Applicant may periodically send an ICMP ping (network management message) and collect the return signal to determine how quickly the message was sent and received; and these collected messages are analyzed using a Kalman filter.

Smith does not teach i) network regulating devices ii) that transmit SNMP messages to a network device

Further, although (as stated above) Applicant does not acquiesce to the Examiner's rejections regarding Smith, in order to expedite prosecution, Applicant has incorporated the subject matter of claims 2 and 3 into claim 1, which now recites the following: "wherein the computing device is a network event regulator device selected from the group of a wireless access point, a switch, a hub, and a router." Also, each of Applicant's independent claims 1, 23 and 39 have been amended herein such that they now recite, in some form, a device including, e.g., a wireless access point, a switch, a hub, and a router that sends an SNMP message to a network device, and receives/collects a response thereto from the network device. It is submitted that these claim revisions are fully supported by the application as filed, at least in (now cancelled) original claims 2, 3, 24 and 27.

This further distinguishes Applicant's claim 1 from Smith because Smith does not anticipate a computing device as now claimed, contrary to the Examiner's assertion. The Examiner cited Smith's access points 180 A-B and paragraph [0049] against Applicant's original claim 3 wherein the computing device includes a wireless access point. Applicant respectfully notes, however, that this is inconsistent with the Examiner citing Smith's 660 as the processor comprising a computing device. Since Smith's processor 660 is outside of access points 180 A-B, Smith's computing device cannot be an access point 180.

Further, Applicant respectfully submits that the Examiner is misinterpreting the Smith reference to state that it anticipates Applicant's recitation regarding transmitting a network management message, using simple network management protocol (SNMP). Smith never mentions SNMP in the cited reference. There is, however, a single reference to an SNMP **Trap** in paragraph [0116] of Smith: "(g) employing a Simple Network Management Protocol (SNMP) Trap".

SNMP is not the same as SNMP Trap, and thus for this additional reason, Smith sending an *alarm* message by SNMP Trap is different from transmitting a *network* *management message* by SNMP transmission. An SNMP message sent by, e.g., a wireless access point, a switch, a hub, a router, etc. (soliciting a response) to a network device is NOT the same as an SNMP Trap sent (unsolicited) by a network device.

SNMP is designed to manage network devices in the Internet and other attached networks. SNMP is the framework used to communicate between the SNMP device (e.g., wireless access point, switch, hub, router, etc.) and the SNMP network device. SNMP Trap is the only message that can be initiated by an SNMP network device. As such, the Examiner is incorrect in stating that a message initiated by a network device (SNMP Trap in Smith) anticipates Applicant's SNMP message sent by its network event regulating device.

Smith does not collect data in response to a network management message

Yet further, Smith's relaying measurement results by a transceiver in response to an alarm message is **not** the same as collecting data that is provided in response to a network management message.

Smith does not teach collecting traffic flow; and teaches away from limiting traffic flow

Regarding independent claim 12, the Examiner attempts to demonstrate that Smith anticipates every element of the claim. The Examiner states "As the bridge 640 monitors traffic it also inherently controls traffic flow from the WLAN 620 to network interface 650." However, Applicant respectfully points out that Smith never states that Bridge 640 monitors traffic. Applicant submits that neither Smith's Bridge 640 nor any other aspect, function, or device disclosed by Smith collects traffic flow amount information from a network device or limits traffic flow through the network device as claimed by Applicant in independent claims 12, 34 and 44. Smith's Bridge 640 transfers traffic. Smith discloses nothing about collecting information about traffic flow amount.

Furthermore, assuming *arguendo*, that the transfer of traffic by Bridge 640 may be read as controlling traffic, it does **not** "limit amount of traffic flow through the network device based on applying the Kalman filter to reduce degraded performance on the network", as recited in Applicant's claim 12 (as well as in claims 34 and 48 that also relate to limiting traffic flow to reduce degraded performance).

Although Smith discloses use of a Kalman filter, the Kalman filter is used to filter data such as position information. Smith applies the Kalman filter to yield a more accurate estimate of the true position (see paragraph [0171] of Smith). In sharp contrast, Applicant applies the Kalman filter to the <u>amount of traffic flow</u>, for example, the number of data points communicated over a period of time. In the Smith example, it is the <u>value</u> of the position data that is filtered, rather than Applicant's filtering the amount of traffic flow. Applying Applicant's terminology to Smith: "amount of traffic flow" would be the <u>number of data points</u>. If Smith <u>limited the amount</u> of traffic flow as recited by Applicant in the relevant pending claims, the result would be a **less** accurate estimate of the true position because fewer data points in a given duration would tend to yield <u>less</u> accuracy—this would destroy Smith's stated purpose.

<u>Claim 34 as presented in the July 7, 2008 was not examined</u>

Yet further, Applicant respectfully points out that the Examiner's remarks related to claim 34 did not accurately quote the claim that was presented as amended July 7, 2008. Applicant submits that "collecting information…" (as quoted in the OA) is **different** from "collecting traffic flow amount information…" (as claimed). Furthermore, the Examiner referenced "regulating external stimuli", but that phrase was deleted in the Amendment filed July 7, 2008. Applicant requests that the Examiner provide a further non-final Office Action examining at least claim 34 as it had been submitted in the response filed July 7, 2008.

<u>Smith does not teach using a Kalman filter to detect abnormality</u>

The Examiner's rejection of claim 5 states that Smith in paragraphs [0167], [0169] and [0171] anticipate controlling and detecting abnormal levels of activity. However, Smith in the cited paragraphs does not discuss "activity". The cited portions of Smith discuss applying Kalman techniques to positioning systems. Smith does **not** discuss using a Kalman filter to detect abnormality. Smith discusses "errors" which are related to position "calculations." It is submitted that Smith does not discuss abnormality because there is nothing <u>abnormal</u> in a positioning system calculation having associated error. Smith's alarms are triggered when the position result of the calculations meets one or more criteria (see Smith, paragraph [0116]). It is submitted that Smith's detecting that a tagged asset has been moved is not an "abnormal level of activity" as claimed by Applicant. Therefore, it is submitted that the citation from Smith does not discuss "program instructions which execute to signal when abnormal levels of activity are detected based on applying the Kalman filter."

For at least all of the above reasons, it is submitted that Applicant's invention as recited in claims 1, 4-23, 25, 26 and 28-49 is not anticipated, taught, or rendered obvious by Smith, either alone or in combination, and patentably defines over the art of record.

35 U.S.C. 103(a) rejection

Claims 6-11, 13-19, 23-33, 35-38, and 35-49 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Smith in view of Narsinh et al. (U.S. Patent Publ. No. 2005/0201415). The Examiner asserts that, "regarding claim 6, Smith teaches a Kalman filter with instructions capable of collecting and analyzing network management information, but fails to specify that the collect of network information includes the step of tracking media access control (MAC) layer addressing and which execute to learn network events based on applying the Kalman filter as other devices connect to the network. Nevertheless, this feature is well known in the art as evidenced by Narsinh. In the same field of endeavor [Applicant takes issue with this statement], Narsinh teaches that MAC addresses are matched in the MAC address tables in an egress and ingress switching device, matching the MAC addresses using the layer 2, a well known process in the art (see Narsinh, par, 0016). Using this technique will facilitate the system in the process of collecting, comparing and analyzing network management information. Accordingly, an average skill in the art [sic], would be motivated [to] incorporate the system of Smith, means of maintaining the advantages reducing the computational demands on the network processor, allowing for improved throughput in switching devices in which the network processor bandwidth is oversubscribed as stated by Narsinh, par. 0003-0004."

Applicant respectfully takes issue with the Examiner's assertion that Smith and Narsinh are in the "same field of endeavor." Smith is a "Wireless position location and tracking system"; whereas Narsinh is "Parallel data link layer controllers in a network switching device." Contrary to the Examiner's assertion above, Smith's asset locator invention is not concerned with, nor does it appear to address oversubscription of network processor bandwidth. As such, it is submitted that one skilled in the art would have no motivation to combine Smith with Narsinh. Indeed, it is submitted that, if the skilled artisan did combine these references in the manner suggested by the Examiner, the stated purpose (asset location) of Smith would be destroyed (as argued above re: **less** accurate estimate of the true position if Smith limited the amount of network traffic flow).

Thus, for at least this reason, it is submitted that the combination of Smith with Narsinh is improper.

Further, assuming *arguendo* that the skilled artisan did combine Smith with Narsinh in the manner suggested by the Examiner, it is submitted that such combination does not render Applicant's invention as recited in claims 6-11, 13-19, 23, 25, 26, 28-33, 35-38 and 35-49. Applicant points out that although Narsinh teaches using MAC layer addressing, Narsinh does not "include[e] program instructions which execute to track media access control (MAC) layer addressing." It is further submitted that Narsinh does not execute program steps which execute to learn network events based on applying the Kalman filter as other devices connect to the network. Since Narsinh does not track the MAC layer addressing, neither Narsinh, nor Smith in view of Narsinh, can base learning network events on applying the Kalman filter as other devices connect to the network.

Yet further, Applicant pointed hereinabove to deficiencies in Smith, and it is submitted that Narsinh does not supply these deficiencies.

For these further reasons, it is submitted that Applicant's invention as recited in claims 6-11, 13-19, 23, 25, 26, 28-33, 35-38 and 35-49 is not anticipated, taught or rendered obvious by Smith in view of Narsinh, and patentably defines over the art of record.

For all the reasons stated above, it is submitted that Applicant's invention as defined in independent claims 1, 12, 23, 34, 39 and 44, and in those claims depending ultimately therefrom, is not anticipated, taught or rendered obvious by the Smith and Narsinh, either alone or in combination, and patentably defines over the art of record.

In summary, claims 1, 4-23, 25, 26 and 28-49 remain in the application. Claims 2, 3, 24 and 27 are cancelled herein without prejudice. It is submitted that, through this Amendment, Applicant's invention as set forth in these claims is now in a condition suitable for allowance.

Further and favorable consideration is requested. If the Examiner believes it would expedite prosecution of the above-identified application, the Examiner is cordially invited to contact Applicants' Attorney at the below-listed telephone number.

Respectfully submitted,

DIERKER & ASSOCIATES, P.C.

/Julia Church Dierker/

Julia Church Dierker
Attorney for Applicants
Registration No. 33368
(248) 649-9900, ext. 25
juliad@troypatent.com

3331 West Big Beaver Rd., Suite 109
Troy, Michigan 48084-2813
Dated: February 17, 2009
JCD/JBD